REMARKS

Applicant thanks the examiner for stating that claims 9-18 are allowable if rewritten in independent form and/or overcoming objections.

The specification has been amended to include section titles, such as "FIELD," "BACKGROUND," "SUMMARY," "DESCRIPTION OF THE DRAWINGS," and "DETAILED DESCRIPTION." Therefore, Applicant respectfully requests that this objection be removed.

Applicant has amended several paragraphs beginning on page 1, line 22 thru page 2, line 22. These paragraphs provide a further overview of the disclosure and do not add new matter.

The Office action states that the drawings are objected to under 37 C.F.R. § 1.83(a). The Office action further states that at least the main features of claims 1-18 must be shown or the features canceled from the claims.

Applicant has included, along with the response, a new FIG. 2 to depict the claim limitations of claims 1-18. No new matter has been added.

The following description provides support for FIG. 2. FIG. 2 is a flow chart of an exemplary access control method performed by the access control system. Each of the operations disclosed in FIG. 2 can be found throughout the originally filed specification. For example, located at the top of FIG. 2 in the first box, the operation states, "Receive access request from apparatus." Support for this operation may be found in the original specification, on at least page 1, line 24, page 4, lines 21-24, page 5, lines 19-23, and, page 10, lines 4-5.

The next operation includes determining whether a unique identification number is provided. Support for this operation may be found in the original specification, on at least page 5, lines 19-23. If the response is "no," the next operation of "send unique identification number in time-limited encrypted cookie file to apparatus" is executed. This operation is supported at least on page 5, lines 19-23. The operation that follows applies "the first access control level." This operation is supported on at least page 5, lines 14-15, page 2, line 3, and page 10, claim 2.

If the unique identification number has been provided, the next operation determines whether the data processing apparatus has been "verified." If verified, the next operation processes the request. This operation is supported at least on page 4, lines 28-30 and page 5, lines 23-31. If not verified, a next operation is executed. In this operation, the first access control level is applied. Support for this operation is located at least on page 5, lines 14-15, page 2, line 3, and page 10, claim 2.

From the operation of apply the first access control level, a next operation includes applying the rate limit to the access request from the apparatus, and is supported at least on page 6, lines 1-15. Once the rate limit is applied to access requests from the apparatus, the next operation determines whether access requests from the apparatus exceed the rate limit, and is supported at least on page 6, lines 10-12. If so, these access requests are queued in the next operation (support is found at least on page 6, lines 10-12).

If the rate limit is not exceeded and/or the access requests are queued, another operation is executed. In this operation, a unique security code, for display on the apparatus, is sent to the apparatus. Support for this operation is found at least on page 4, line 29 – page 5, line 2, page 5, lines 23-31, and page 10, claims 1 and 3. After the unique security code is sent to the apparatus, the next operation calls the telephone of the user from the IVR and prompted for security code. Support for this operation is found at least on page 5, lines 23-26. The next operation determines whether the security code has been received correctly, and is supported, at least on page 5, line 27-29. If yes, the next operation indicates that the security code is verified (support is found at least on page 5, lines 27-29) and an additional operation that includes processing the access request.

If security code is not correctly received from the IVR, a next operation including advancing to the next access control level is executed. This operation is supported at least on page 4, lines 8-19, page 6, lines 27-30, page 7, lines 1-4, and page 10, claim 2. The next operation includes applying the hack detection tests, if the current control level is the second control level. This operation is supported at least on page 2, line 5-6, page 4, line 17-18, and page 12, claim 14.

If the current control level is not equal to the second control level, a next operation is executed. In this operation, the system downloads code to the apparatus for encrypting communication, if the current control level is equal to the third access level. Support for this operation may be found page 4, lines 16-19 and page 8, lines 9-24. If the current control level is not equal to the third control level, the next operation executes to block the IP address or segment related to the apparatus. This operation is supported on page 4, line 18-20, page 8, line 31 – page 9 line 6, page 11, claim 11.

If the current control level is equal to the second access control level or the third access control level, another operation is executed. In this operation, the system determines whether the access control level of time has expired. If yes, the system executes another operation that moves the current access level to the previous access level. This operation is supported at least on page 8, lines 4-7 and 26-29. If the access control level time has not expired, the system continues to execute check whether the control level time has not expired, and is supported at least on page 6, line 25-29.

In addition to the main claimed limitations being disclosed in FIG. 2, Applicant also states that FIG. 2 does not add any new matter. Therefore, Applicant respectfully requests that this objection be removed.

The Office action states that Claim 18 is objected to for a number of informalities. Claim 18 has been amended to recite "providing the identification data received" in order to specify the data. Additionally, Applicant has deleted the "IVR" abbreviation in line 5 of the claim, and added the terms "interactive voice response system." Therefore, Applicant respectfully requests that the Examiner to remove this objection.

Claim 18 has been objected to because, line 6 recites "...and providing the data received..." which does not specify the data. Applicant has amended the claim, in line 6, to recite "...and providing the identification data received...." Therefore, Applicant respectfully requests the Examiner to withdraw this objection.

Claims 1, 5, 14, and 18 have been rejected under 35 U.S.C. § 112, second paragraph.

Claims 1 has been amended to recite "applying a rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system." (emphasis added) Applicant believes that this limitation is clear and meaningful. Therefore, Applicant respectfully requests the Examiner to withdraw this rejection.

Claims 14 and 18 have been similarly amended. Therefore, Applicant respectfully request the Examiner to withdraw this rejection.

Claim 1 has been amended to recite that the "said identification data is received from a user of said apparatus and verified by said access control system." Applicant, therefore, respectfully requests that the Examiner withdraw this rejection.

Claim 5 states that "the identification data is verified by said user returning said identification data using independent communication means having a known association to said user and said data processing apparatus." As supported by the specification on page 4, line 29 – page 5, line 2, this operation is a part of the verifying process of the access control method. Therefore, Applicant respectfully requests that the Examiner withdraw this rejection.

The Office action states that Claims 1, 14, and 18 recite "rate limit," but these claims neither specify the object of the applied rate limit nor the nature of the rate limit. Applicant has amended claim 1 to recite "applying a rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system." Claims 14 and 18 have been similarly amended. Therefore, Applicant respectfully requests the Examiner to withdraw these rejections.

Claim 14 has been amended to include the actions performed. Therefore, Applicant believes that claim 1, 5, 14, and 18 are now in compliance with 35 U.S.C. § 112, first paragraph, and respectfully request the Examiner to remove these rejections.

Claims 1, 14, 18 have been rejected under 35 U.S.C. § 112, first paragraph. Claim 1 has been amended such that at least one operation includes "applying a rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system" which is enabled by the specification. Claims 14 and 18 have been similarly amended. Therefore, Applicant respectfully request the Examiner to remove these rejections.

Claim 1 is rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Applicant has amended claim 1 to include "applying a rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system." In the claimed invention, the access control system receives an access request for a service from a data processing apparatus. In response to the access request, the access control system sends unique identification data to the apparatus. The access control system places the access request in an access request queue until the identification data is received from a user of the apparatus. Applicant, therefore, believes that this amendment specifies a known result, such that the access request is placed in an access request queue until the identification data is received from the user and verified by the access control system. Therefore, Applicant respectfully requests that the Examiner remove and withdraw this rejection.

Claims 1-8, 16 and 17 are rejected under 102(e) as being anticipated by Guthrie et al.

Guthrie et al. disclose a personal authentication system. See Abstract. If the system employs a conventional first level of authentication, the user 114 initially inputs the user's account and correct password to the client 102. Col. 7, lines 15-17. The client 102, via the client application 112, transmits the user account and account password to the server 104. Col. 7, lines 17-19. The server 104 validates the user account and password against the user's account table stored in the user account database 120. Col. 7, lines 19-21. If such initial validation is successful, the server 104 employs a change generator in its Secure Authentication Database (SADB) calculator 116 to generate a challenge 126, and transmits the challenge to the client 102. Col. 7, lines 21-26. The client SADB calculator prompts the user for the user's SADB password, which the user enters into the client 102. Col. 7, lines 27-29. Additionally, the user 114 enters the received challenge into the client SADB calculator 110. Col. 7, lines 26-28. The client SADB calculator 110 generates the response using the challenge, SADB password, and the locally stored serial number. Col. 7, lines 34-37. The server SADB calculator employs a compare routine to compare the received response with the response locally generated by the server 104. Col. 7, lines 38-41. The server 104 provides the client 102 with a message indicating whether the authorization succeeded or failed, and enables appropriate access if successful. Col. 7, lines 41-43.

Amended claim 1 is patentable over the Guthrie et al., since Guthrie et al. do not disclose an operation of "applying a rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system." In contrast, Guthrie et al. appears to first authenticate a user on the basis of a received account identifier and password. Once the user is authenticated, then a second level access control is employed involving a challenge/response process.

More specifically, Guthrie et al. appears to disclose an authentication process where the server sends a challenge and receives a response generated based on a user's password, a unique serial number, and the challenge. Col. 4, lines 19-22. The server's calculator locks out a user and denies access after a certain number of failed attempts and denies access for a certain period of time. Col. 4, lines 29-32. This limit imposed by the challenge/response process of Guthrie et al. appears to be a complete denial of access for a certain period of time when an incorrect response is received. As stated in claim 1, on the other hand, the present invention allows access for verification, but a rate limit is imposed using an access request queue until verification. This allows multiple users to attempt to use identification credential without affecting each other.

Additionally, Guthrie et al. appears to send a challenge to a data processing apparatus, i.e. a client computer, which involves sending a seed value. Col. 4, lines 16-19. The seed value is processed with a unique serial number and the authentication password to generate the response. Col. 4, lines 20-22. However, claim 1 refers to sending the unique identification data to the apparatus and it is this data itself that is to be received from a user before verification can occur. Also, as recited in dependent claims, an independent device is used by the user to provide identification data.

Guthrie et al. appears to apply a limit that locks out an authenticated user and denies access to the authenticated user after a number of failed attempts. Col. 4, lines 30-35. As stated in amended claim 1, the present invention, on the other hand, will allow a verified user to continue to have access, and only applies a rate limit to an apparatus when a user is not verified. Additionally, Guthrie et al. appears to allow the same machine to continually gain access merely by using different user data. On the other hand, in the present invention it is a particular machine, based on address data or unique identification number, that may be blocked, not a user.

Guthrie et al. does not appear to apply to anonymous users or users seeking to use the same credentials; whereas the present invention is able to deal with both.

Therefore, for the reasons stated above, Applicant believes that claim 1 is patentable under 35 U.S.C. § 102(e) over the applied reference.

Claims 2-8, 16 and 17 depend on claim 1 and are patentable for the same reasons as Claim 1 and by reason of additional limitation called for therein.

New Claims 19-23 and 25-26 depend from claim 1 and are patentable for the same reasons as claim 1 and by reason of additional limitations called for therein.

New claims 19 and 27 depend from claim 14 and are patentable for the same reasons as claim 14 and by reason of additional limitations called for therein.

New claims 24 and 28 depend from claim 18 and are patentable for the same reasons as claim 18 and by reason of additional limitations called for therein.

In view of the foregoing, it is respectfully submitted that the claims of record are allowable and that the application should be passed to issue. Should the Examiner believe that the application is not in a condition for allowance and that a telephone interview would help further prosecution of this case, the Examiner is requested to contact Edward N. Bachand at the phone number below.

Respectfully submitted,
DORSEY & WHITNEY LLP

Lee R. Osman
Reg. No. 38,260

Customer No. 32,940
US Bank Centre
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010
Telephone No.: (650) 857-1717
Facsimile No.: (650) 857-1288

4847-0554-5729\3